

Packet Tracer Lab 2 Solution Guide

DNS Resolution Failure Investigation

Incident ID: INC-1002

Objective

This lab focuses on identifying and resolving a DNS resolution issue affecting multiple users within a small office environment.

Users are unable to access websites and cloud-based resources following scheduled maintenance activities performed earlier in the day.

The objective is to troubleshoot the issue using a structured methodology, identify the root cause, restore DNS functionality, and validate successful name resolution.

Root Cause

The DHCP pool **OFFICE** assigns an incorrect DNS server (**8.8.8.250**) instead of the correct DNS server (**8.8.8.10**).

Symptoms Observed

- Website access unavailable
- DNS resolution failing
- Local device communication functional
- External IP connectivity functional
- Devices receiving IP addresses successfully
- Browser connectivity failing
- Multiple departments affected

BridgeOpsOne

Troubleshooting Process

1. Attempt to reach the website.

```
ping bridgeopsone.com
```

The ping should fail.

2. Verify local connectivity.

```
ping 192.168.10.1
```

The ping should succeed.

3. Verify external IP connectivity.

```
ping 8.8.8.10
```

The ping should succeed.

4. Review the workstation's DHCP configuration.

```
ipconfig /all
```

Observe the assigned DNS server.

5. Test communication to the assigned DNS server.

```
ping 8.8.8.250
```

BridgeOpsOne

The ping should fail.

6. Review the DHCP pool configuration.

```
show running-config
```

Locate the DHCP pool and identify the incorrect DNS server assignment.

Commands Used

```
ipconfig /all  
ping bridgeopsone.com  
show running-config  
show ip dhcp pool  
ipconfig /release  
ipconfig /renew
```

Resolution

```
conf t
```

```
ip dhcp pool OFFICE
```

```
no dns-server 8.8.8.250
```

```
dns-server 8.8.8.10
```

```
end
```

```
write memory
```

BridgeOpsOne

Then renew the DHCP lease.

```
ipconfig /release
```

```
ipconfig /renew
```

```
ipconfig /all
```

Verify the workstation now receives DNS server:

8.8.8.10

Validation

Successful resolution should include:

- Ping 192.168.10.1 succeeds.
- Ping 8.8.8.10 succeeds.
- Ping bridgeopsone.com succeeds.
- Client receives 8.8.8.10 as the DNS server after DHCP renewal.
- Website loads successfully in the browser.

Key Takeaways

- Follow a structured troubleshooting methodology.
- Validate connectivity before assuming a DNS issue.
- Successful IP connectivity does not guarantee successful name resolution.
- DHCP distributes critical DNS information to clients.
- Incorrect DNS settings can appear as complete internet outages.
- Troubleshooting should isolate each layer before identifying the root cause.

Known Behavior

After modifying the DHCP pool, existing clients may continue using the previous DNS server until they renew their DHCP lease.

If validation fails after correcting the DHCP configuration, renew the client lease using:

```
ipconfig /release
```

```
ipconfig /renew
```

BridgeOpsOne

or toggle the workstation from Static back to DHCP in Packet Tracer.